An Initial Industrial Cybersecurity Workforce Development Framework

Sean McBride
La Trobe University
S.McBride@latrobe.edu.au

Corey Schou
Idaho State University
schou@niatec.iri.isu.edu

Jill Slay
University of South Australia
Jill.Slay@unisa.edu.au

Abstract

This document discusses the research methodology and outcomes of an effort to create a simple, flexible framework for developing an industrial (ICS) cybersecurity workforce. The effort used a variation of the nominal group technique relying on subject matter experts from the Idaho National Laboratory to develop five archetypal job roles: industrial cybersecurity technicians, engineers, analysts, researchers, and managers. We propose that these archetypes require additional contextual (non-cybersecurity) knowledge grouped into six areas: industrial processes & operations; instrumentation & control; equipment; communications; safety; and guidance & regulation. We note that this approach offers advantages over other cybersecurity workforce frameworks, and recommend future work to elaborate tasks performed by these roles relying on the identified knowledge areas, as well as to explore the applicability of the archetype approach to aid workforce development in other specialized cybersecurity contexts.

1. State of Industrial Cybersecurity Workforce Development

Several workforce studies over the past years, such as [1-3], indicate great need for cybersecurity professionals. We note that while industrial cybersecurity (dealing with industrial control systems [ICS] environments) represents a small quantity of this growing need, the pace of technological innovation that couples information systems with process control systems, and significant consequences of actual industrial cybersecurity events, will require many more of these professionals [4-5].

Authors of [6] explain that merely adapting existing cybersecurity educational approaches to industrial cyber-physical environments falls short on three fronts:

- *Foundational information security concepts were created without consideration for the unique needs of industrial control environments.*
- *Existing educational standards for ICS security lack thorough development.*
- *Current standards do not account for the career paths of industrial professionals.*

Authors of [7] demonstrate that existing curricular guidance and workforce development frameworks do not meet a set of reasonable criteria to achieve consideration as an industrial cybersecurity workforce development and training standard.

2. Methodology

2.1 Impetus

As a National Laboratory with special interest in protecting critical industrial control systems from cyber-attacks and events, the Idaho National Laboratory (INL) employs hundreds of professionals working across the fields of industrial systems, critical infrastructure, and cybersecurity [8]. Recognizing the need for a clear internal workforce development framework for industrial cybersecurity personnel, Laboratory leadership engaged the authors to develop a prototype framework that might also be useful to other organizations facing similar workforce needs.

2.2 Historic Contribution to Cybersecurity Education Standards

Idaho State University has a deep, if often unrecognized, history of leadership in cybersecurity education and training. In the late 1980s, Dr. Corey Schou and a handful of colleagues hosted a series of workshops that produced some of the first educational materials for information security including the 409-page "Comprehensive Information Assurance Dictionary' [18] and 326-page "Integrating Information Security" modules [19-20].

Beginning in 1987, the National Security Agency (NSA) in cooperation with the Federal Information Systems Security Educators Association (FISEEA) funded an expert session at ISU with the mission of creating the first US federal government standard for information systems security education. This work [21] resulted in the publication of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-16, published in 1998 [13].

Between 1991 and 2005, the NSA, under the guidance of W. Victor Maconachy, Michael Jacobs, and Richard Marshall – and influenced by Richard Clarke at the Whitehouse – engaged the Informatics Research Institute at ISU to host additional sessions to deepen and elaborate the original work, moving from general knowledge to specific roles. The output of these sessions became the National Security Telecommunications and Information Systems Security (NSTISS) – later known as the Committee on National Security Systems (CNSS) – Instructions 4011-4016. Table 1 displays the numbers and titles of these documents as well as their formal release dates. It should be noted that documents CNSSI 4012 and 4014 replaced NSTISSI documents of the same number, and that both NSTISSI documents were dated August 1997 [10].

Table 1. Development of National Cybersecurity Education and Training Standards

Document	Title	Study Start	Release Date
NSTISSI 4011	National Training Standard for Information Systems Security (INFOSEC) Professionals	1991	06/20/1994
CNSSI 4012	National Information Assurance Training Standard for Senior Systems Managers	1993	06/01/2004 First Rel 08/1997
CNSSI 4013	National Information Assurance Training Standard For System Administrators (SA)		03/01/2004
CNSSI 4014	Information Assurance Training Standard for Information Systems Security Officers		04/01/2004 First Rel 08/1997
NSTISSI 4015	National Training Standard for Systems Certifiers		12/01/2000
CNSSI 4016	National Information Assurance Training Standard For Risk Analysts		11/01/2005

These Instructions formed the basis for training federal employees in the field of information assurance. Our interpretation is that to leverage existing academic institutions to produce the information security personnel required for government agencies to fulfill their national security missions, the NSTISSC, with NSA in its role as secretariat, could not wait for traditional academic accrediting bodies, such as ABET, and opted to create its own set of curricular examples and criteria.

By demonstrating compliance with these criteria, schools could qualify for designation as a "Center of Academic Excellence (CAE)" in Information Assurance (now Cybersecurity) [11-12].

2.3 Simplot Decision Support Center and the Nominal Group Technique

The Simplot Decision Support Center (SDSC) is an in-person electronic meeting room located on the fourth floor of Idaho State University's Business Administration building. The Center, as a small, 15-seat amphitheater, was designed to implement the nominal group technique for decision making, which technique Van Den Ven and Delbecq report effectively elicits diverse perspectives [14-15].

The technique requires synchronous deliberations be held in writing, anonymously, and in vocal silence. These criteria work to counteract dominant personalities, pre-existing political relationships, and social pressure, thereby enhancing group effectiveness. In the Center, each participant can view their own monitor, the group display at the front of the room, and the moderator. They cannot view the monitor used by other participants [9].

Schou and Frost – who have implemented the technique in the SDSC hundreds of times – empirically report that the technique places significant pressure on the moderator to carry the group through a decision-making process that achieves the objective. As such, it is important that the moderator have a strong understanding of the decision-making process, including approaches and options to give participants, know the software well, display general familiarity with the subject matter, and suspend his or her own bias. They find an assistant moderator particularly useful in simultaneously performing these tasks.

Prior to the session, the moderator reviews the objective of the session, and prepares a rough script of the questions the group intends to address. The moderator uses a set of techniques, such as brainstorming, nominations, rankings, and voting to guide the process.

It is important to note that the SDSC is a decision support center. The participants themselves are not subjects of study, but collaborate by imparting what they know to address a specific issue. Software used in the SDSC produces an anonymous log of the input and records the decisions made by the group.

3. Session Narrative

On February 12, 2019, the INL sent 14 subject matter experts to Idaho State University to use the SDSC with the objective of creating a framework for developing industrial cybersecurity education and training standards.

The group's professional background included titles such as Power Plant Operator, HVAC Specialist, Field Electrician, Information Security Technology Officer, Computer Technology Analyst – SCADA, ICS, and Cybersecurity Consultant, among others. The group's former employers included Northern California Power Agency, Raytheon, National Security Agency, Virginia Transformer, El Paso Electric, and Phillips 66, among others. In total, the group reported 31 years experience in industrial cybersecurity, 32 years in non-ICS information security, and 88 years in industrial operations.

At about 8:30 a.m. the group filed into their seats in the SDSC. Participants heard introductory comments from Dr. Corey Schou, University Professor of Informatics, ISU; and Scott Cramer, Directory of INL's Cybercore Division. The participants then introduced themselves to one another.

Dr. James Frost, who served as moderator for all of the previous NSA-sponsored information assurance education and training standards development sessions, took the moderator's chair for this session.

The group first engaged in a warm-up brainstorming exercise intended to stimulate mental activity relevant to the topic, and introduce them to the software with its flow of written interaction. The warm-up centered on the question, "how does industrial cybersecurity differ from standard information security?"

Following the warm-up exercise the group addressed the issue: What job roles exist in the field of industrial cybersecurity? The group identified 81 separate job titles, which it then organized into five categories: Technician, Engineer, Analyst, Researcher, and Manager. Five titles were not easily assigned to these groups, and were set aside for future investigation. When asked to pick which two categories were most important to elaborate, the group chose first, Engineer, and second, Technician.

The group then addressed "what knowledge does an ICS security professional need to know that is not covered in standard information security?" The group identified 86 terms and concepts, which it organized into five categories: Industrial Processes & Operations; Instrumentation & Control; Equipment; Communications; Safety; Guidance & Regulation. The group recognized that this final category would exist in standard information security, but the contents of this category would be different.

Unfortunately, participants were not asked which of these groups would be most important to elaborate first. However, recognizing the group's reported 88 years combined experience in industrial operations, we believe it would have been Safety

After lunch, the group spent a taxing session in which it mapped verbs from Bloom's taxonomy [16] to the knowledge list generated in the morning. While this process mirrored that used in NSA sessions to create the 4011-4016, the experts expressed concerns over possible incompleteness of the knowledge list produced,

it's unclear connection to cybersecurity tasks, and the monotony of producing the mapping.

4. Results and Analysis

The key contributions of this session were the identification of the five Archetype Roles and the six Knowledge Areas for industrial cybersecurity professionals

4.1. Archetype Roles

An archetype role represents a prevailing job category. Actual job titles within that category may vary to a certain degree, as may associated tasks (which were not developed during this session). The major benefit of archetype roles is their intuitive simplicity:

- Those with limited workplace experience or domain expertise, such a high school student or even an average citizen, may at least notionally recognize differences among a manager, an analyst, and a technician.
- The use of archetypes bypasses potential convolution associated with using security-specific duties as primary categories, (which we note is the approach used by the CNSS Instructions, and the NIST NICE framework [10, 13]).
- Reliance on these simple roles may help bake cybersecurity into existing positions rather than overtly promoting separate cybersecurity specialists (while leaving the door open to the latter), which we view as a significant need.
- We also feel that five is a manageable number of archetype roles.

Our chief concern related to the archetype roles is that individuals or organizations attempting to apply them may consider them to be specifically prescriptive rather than notionally prescriptive. We warn against this misuse, as we wish to preserve the ingenuity and flexibility of employers to meet their own workforce needs.

4.2. Knowledge Areas

A knowledge area is a noun category that represents what a professional would need to know to reasonably function within a field. In this case the field is the industrial aspect of industrial cybersecurity. We intended the knowledge areas to roughly apply across all archetype job roles. Because these are categories, the most significant concepts – such as those that most importantly differentiate industrial cybersecurity from information security – may occur within a category.

We note that the US Department of Labor, working with the International Society of Automation (ISA) and its Automation Federation produced an Automation Industry Competency model, which defines 5 industry-wide technical competencies, and an additional 7 industry-sector technical competencies [17]. The document itself recognizes these competencies occur at different levels; hence, we recognize natural overlap between the 5 and the 7, and assert that the 6 we identified is not inconsistent with this previous work. We feel confident that 6 is a reasonable number.

5. Future Work

As noted above, this effort did not produce a task list for industrial cybersecurity archetype roles. For this, we recommend alternate methods, such as focus groups, surveys, interviews and field observations where participants have appropriate experience in the industrial cybersecurity archetype roles; likewise, the content of the knowledge areas requires additional elaboration, which we suspect can be obtained from existing documents and input of participants with appropriate experience in the industrial cybersecurity archetype roles.

In future work, we intend to explore the applicability of the archetype approach to aid workforce development in other specialized cybersecurity contexts.

6. References

[1] Center for Strategic and International Studies, “Hacking the Skills Shortage”, McAfee, Santa Clara, CA, July 2016. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf. Accessed June 10, 2020.

[2] Frost & Sullivan, “2017 Global Information Security Workforce Study”, 2017. https://www.iamcybersafe.org/s/gisws. Accessed June 10, 2020

[3] (ISC)2, “Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens”, 2018. https://www.isc2.org/-/media/ISC2/Research/2018-ISC2-Cybersecurity-Workforce-Study. Accessed June 10, 2020.

[4] D. Oliver and M. Haney, "Preparing the next cyber-resilient workforce through cross-pollination education," 2017 Resilience Week (RWS), Wilmington, DE, 2017, pp. 44-49, doi: 10.1109/RWEEK.2017.8088646.

[5] National Academies of Sciences, Engineering, and Medicine, “A 21st Century Cyber-Physical Systems Education” Washington, DC: The National Academies Press, 2016. https://doi.org/10.17226/23686.

[6] S. McBride and J. Slay “Towards Standards-Based Industrial Control Systems Security Education in The United States”, 2020. https://industrialcyberforce.org/wp-

content/uploads/2020/07/Towards-Standards-based-ICS-Security-Education-in-the-United-States.pdf. Accessed July 7, 2020.
[7] S. McBride and J. Slay "Criteria for International Industrial Cybersecurity Education and Training Standards". 2020. https://industrialcyberforce.org/wp-content/uploads/2020/07/Criteria-for-International-ICS-Security-Education-Standards.pdf. Accessed July 7, 2020.
[8] Idaho National Laboratory. "General Information", (n.d.). https://inl.gov/about-inl/general-information/. Accessed June 10, 2020.
[9] Idaho State University, "Simplot Decision Support Center", (n.d.). http://cobhomepages.cob.isu.edu/schou/SDSC.htm. Accessed June 10, 2020.
[10] Committee on National Security Systems, "Instructions", (n.d.). http://www.cnss.gov/CNSS/issuances/Instructions.cfm. Accessed June 10, 2020.
[11] M. Bishop and C. Taylor, "A Critical Analysis of the Centers of Academic Excellence Program", 2009. https://cisse.info/resources/archives/category/12-papers?download=125:s01p04-2009
[12] National Security Agency, "National Centers of Academic Excellence", (n.d.). https://www.nsa.gov/resources/students-educators/centers-academic-excellence/. Accessed June 11, 2020
[13] National Institute of Standards and Technology, "Special Publication 800-16 Information Technology Security Training Requirements: A Role- and Performance-Based Model", 1998. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-16.pdf. Accessed June 10, 2020.
[14] Delbecq, A. L., Van de Ven, A. H., & Gustafson, D. H. "Group techniques for program planning : a guide to nominal group and Delphi processes." Scott, Foresman, 1975.
[15] Van de Ven, A. H., & Delbecq, A. L. "The Effectiveness of Nominal, Delphi, and Interacting Group Decision Making Processes. Academy of Management Journal, 17(4), 605–621, 1974. https://doi-org.libpublic3.library.isu.edu/10.2307/255641. Accessed June 11, 2020.
[16] Bloom, B., et al. as described by University of Toronto. "Appendix B: Useful Verbs for Developing Learning Outcomes", (n.d.). https://teaching.utoronto.ca/teaching-support/course-design/developing-learning-outcomes/appendix-b-useful-verbs-for-developing-learning-outcomes/. Accessed June 11, 2020.
[17] U.S. Department of Labor, "Automation Industry Competency Model V. 4", 2009 (updated 2018). https://www.careeronestop.org/CompetencyModel/competency-models/pyramid-download.aspx?industry=automation. Accessed: June 5, 2020.
[18] C.D. Schou and J. Frost, "Comprehensive Information Assurance Dictionary", 1988.
[19] C.D. Schou., J. Frost, N. Wingert, J. Larsen, H. LaFond, E. Munson, "Integrating Information Security" from Simplot Decision Support Center Report 162, 1989-2001.
[20] E. Spafford, "An Anniversary of Continuing Excellence", 2019. https://www.cerias.purdue.edu/site/blog/2019/05/. Accessed June 2020.
[21] C. D. Schou, W. V. Maconachy, and J. Frost. "Developing Awareness, Training and Education: A Cost Effective Tool for Maintaining System Integrity", In Proceedings of the IFIP TC11, Ninth International Conference on Information Security: Computer Security (IFIP/Sec '93). North-Holland Publishing Co., NLD, 53–63, 1993.

Acknowledgements

This work was supported by a Scholarship from La Trobe University.

The Authors acknowledge the significant contributions of 14 subject matter experts from the Idaho National Laboratory.